**DEPARTMENT OF THE NAVY**
**HEADQUARTERS UNITED STATES MARINE CORPS**
**3000 MARINE CORPS PENTAGON**
**WASHINGTON, DC 20350-3000**

IN REPLY REFER TO:
5500
ARS
OCT 04 2011

Security Note 06-11

From: Director, Administration and Resource Management Division
To: Security Coordinators

Subj: GUIDANCE ON THE PROPER USE OF MOBILE CRYPTOGRAPHIC EQUIPMENT

Ref: (a) OPNAVINST C5510.93F/MCO 5510.19, Navy/Marine Corps Implementation of National Policy on Control of Compromising Emanations
(b) Department of the Navy SME PED User Agreement
(c) EKMS 1 (series), Ch 5 sub 530 and 535, Ch 9 sub 930 c.

1. Introduction. In accordance with the references the following guidance shall be adhered to when using the Secure Mobile Environment for Portable Electronic Devices (SME/PED)'s, mobile suites (which include cryptographic equipment, i.e. KG 175D, KG 235, etc.), and other devices capable of sending, receiving audio and visible classified data (i.e. Secure IPad, IRIDIUM phones in secured mode, GSM secure cell phones, portable SIPRNET printers, SIPRNET laptops) in areas designated **not safe** for exploitation of compromising emanations (CE).

2. Background. In accordance with reference (a), the existence and study of the nature of CE are referred to as TEMPEST, which is a code word used to describe the unintentional data-related or intelligence-bearing signals. If these signals are intercepted and analyzed, they could disclose the information transmitted, received, handled, or otherwise processed by electrical information-processing equipment or systems. Any type of electrical information-processing device whether an ordinary electric typewriter or a large complex data processor, may produce CE. Although comprehensive national threat evaluations are performed on a continuing basis to identify the nature and extent of the TEMPEST threat, foreign governments are actively engaged in attacks against U.S. secure communications and other information processing facilities for the expressed intention of exploiting CE.

3. Usage. The SME/PED, mobile suites, and other mobile devices allow the mobility and accessibility of classified information. It is easy to unintentionally disregard the vulnerability factors that are present, but it is the user's responsibility to always remain alert. This document will provide guidance on the processing, conversing, reading or viewing of National Security Information in public and private spaces (i.e. hotel conference rooms or any other location not approved to store or transmit classified information).

4. Safeguarding. Protect all equipment and material based on its classification. Users of SME/PEDs, mobile suites and other devices that are capable of sending, receiving, viewing, and hearing classified data (i.e. Secure IPad, Iridium Phones in secure mode, portable SIPRNET printers) are reminded that it is the users' responsibility to ensure it is mission essential to use equipment when in public and private spaces. When required

to use devices, individuals should isolate themselves from the general public and ensure sufficient privacy is available to allow the equipment to be used in classified mode with minimal risk of compromise, eaves-dropping, and/or viewing by unauthorized individuals. Individuals are reminded to be continuously observant of their surroundings when using classified mobile devices. However, the use of cryptographic equipment (i.e. KG 175, KG 235) is strictly prohibited in public and private spaces (i.e. hotel conference rooms or any other location not approved to store or transmit classified information).

5. Traveling. Adherence to reference (b) and (c) are imperative while traveling with these mobile devices. Furthermore, users must ensure that SME/PEDs and other mobile secure devices are logged off and in the unclassified mode when being x-rayed, physically/visually examined at installation entry points, in-flight, and other similar locations where such devices are routinely inspected, and may be powered on when requested in the unclassified mode. The user should not surrender the device for x-raying or inspection when the device is in the classified mode. If cryptographic equipment is shipped it must be in the unclassified mode, unkeyed, and double wrapped.

6. Storage. Store devices in GSA containers and spaces approved for their storage unless material or devices are under the direct sight and control of authorized persons. When traveling outside the National Capital Region, foreign countries, and/or to areas where threat levels are elevated and pose higher risks to enemy exploitation activity, it is imperative to have two couriers and to plan ahead by contacting and utilizing available U.S. embassies or U.S. military controlled installations to store and process classified information, material, and/or equipment.

7. COMSEC Incident Reporting. In accordance with reference (c), immediately notify the EKMS Manager and Command Security Manager of any suspected tampering, access by unauthorized personnel, loss, theft, unattended devices, or actions that caused or required the device to be zeroized or destroyed.

8. Questions regarding this Security Note should be directed to Mr. Isaac Encarnacion, at (703) 614-2305, or email: isaac.encarnacion@usmc.mil.

R.J. Geberth
R. J. GEBERTH
By direction

Copy to:
ARS
Files